

Київський національний університет імені Тараса Шевченка
Факультет комп'ютерних наук та кібернетики
Кафедра системного аналізу та теорії прийняття рішень

Звіт
з лабораторної роботи № 1
на тему:
«Генерування псевдовипадкових чисел»

Студента другого курсу
групи К-23(2)
Міщука Романа Андрійовича
Факультету комп'ютерних наук
та кібернетики

1. Опис методів генерування рівномірно розподілених чисел

1. Лінійний конгруентний метод

$$X_{n+1} = (aX_n + c) \bmod m,$$

$$U_{n+1} = \frac{X_{n+1}}{m}, n \geq 0,$$

де m – модуль, $m > 0$, a – множник, $0 \leq a < m$, c – приріст, $0 \leq c < m$, X_0 – початкове значення, $0 \leq X_0 < m$.

Вибір модуля. Модуль повинен бути достатньо великим, оскільки період не може містити більше m чисел. Нехай w – довжина комп'ютерного слова, наприклад, 2^{32} . В якості m рекомендується брати найбільше просте число, яке не перевищує w .

Вибір множника. Цей вибір визначається наступною теоремою: лінійна конгруентна послідовність, визначена числами m , a , c і X_0 має період m тоді і лише тоді, коли виконуються три умови:

1. числа c і m є взаємно простими;
2. число $b = a - 1$ є кратним числу p для кожного простого числа p , яке є дільником числа m ;
3. число b є кратним 4, якщо число m є кратним 4.

Обрані коефіцієнти:

- $X_0 = 42949672$;
- $m = 4294967291$;
- $c = 4294967279$;
- $a = 4294967231$.

Результат роботи:

```
C:\Users\mario\Documents\Documents\University\OOP\LABS\LAB1\Release\LAB1.exe
Enter index of method (from 1 to 10 or q): 1
Chose one of the presets, or enter own numbers:
1) m1_31b
2) m1_32b
3 or d) m1_p
o) Own numbers
:d
Enter number of elements: 1000
Interval | Frequency
[0.00;0.10) 0.09
[0.10;0.20) 0.12
[0.20;0.30) 0.11
[0.30;0.40) 0.10
[0.40;0.50) 0.10
[0.50;0.60) 0.08
[0.60;0.70) 0.09
[0.70;0.80) 0.11
[0.80;0.90) 0.10
[0.90;1.00) 0.10
Enter index of method (from 1 to 10 or q): _
```

2. Квадратичний конгруентний метод

$$X_{n+1} = (dX_n^2 + aX_n + c) \bmod m,$$

$$U_{n+1} = \frac{X_{n+1}}{m}, n \geq 0.$$

Вибір параметрів. Цей вибір визначається наступною теоремою: квадратична конгруентна послідовність, визначена числами m, a, c, d і X_0 , має період m тоді і лише тоді, коли виконуються чотири умови:

1. числа c і m є взаємно простими;
2. числа d і $a-1$ є кратними числу p для всіх чисел p , які є простими непарними дільниками числа m ;
3. число d є парним і $d \equiv a-1 \pmod{4}$, якщо число m є кратним 4; число $d \equiv a-1 \pmod{2}$, якщо число m є кратним 2;
4. $d \not\equiv 3c \pmod{9}$, якщо число m є кратним 3.

Обрані коефіцієнти:

- $X_0 = 42949672$;
- $m = 4294967291$;
- $c = 4294967279$;
- $d = 4294967231$;
- $a = 4294967197$.

Результат роботи:

```
C:\Users\mario\Documents\Documents\University\OOP\LABS\LAB1\Release\LAB1.exe
Enter index of method (from 1 to 10 or q): 2
Chose one of the presets, or enter own numbers:
1) m2_32b
2 or d) m2_p
o) Own numbers
:d
Enter number of elements: 1000
Interval    | Frequency
[0.00;0.10)  0.11
[0.10;0.20)  0.12
[0.20;0.30)  0.11
[0.30;0.40)  0.08
[0.40;0.50)  0.10
[0.50;0.60)  0.09
[0.60;0.70)  0.10
[0.70;0.80)  0.10
[0.80;0.90)  0.10
[0.90;1.00)  0.11
Enter index of method (from 1 to 10 or q):
```

3. Числа Фібоначчі

$$X_{n+1} = (X_n + X_{n-1}) \bmod m, n \geq 0.$$

Обрані коефіцієнти:

- $X_0 = 1247437$;
- $X_1 = 224743647$;
- $m = 4294967291$.

Результат роботи:

```
C:\Users\mario\Documents\Documents\University\OOP\LABS\LAB1\x64\Release\LAB1.exe
Enter index of method (from 1 to 10 or q): 3
Chose one of the presets, or enter own numbers:
1 or d) m3_p
o) Own numbers
:d
Enter number of elements: 1000
Interval    | Frequency
[0.00;0.10)  0.10
[0.10;0.20)  0.11
[0.20;0.30)  0.10
[0.30;0.40)  0.10
[0.40;0.50)  0.10
[0.50;0.60)  0.09
[0.60;0.70)  0.09
[0.70;0.80)  0.10
[0.80;0.90)  0.11
[0.90;1.00)  0.09
Enter index of method (from 1 to 10 or q): _
```

4. Обернена конгруентна послідовність

$$X_{n+1} = (aX_n^{-1} + c) \bmod p,$$

$$U_{n+1} = \frac{X_{n+1}}{m}, n \geq 0,$$

де p – просте число, число X_n набуває значень із множини $\{0, 1, \dots, p-1, \infty\}$, а обертання визначається за правилами $0^{-1} = \infty$, $\infty^{-1} = 0$. В інших випадках $XX^{-1} \equiv 1 \bmod p$.

Вибір параметрів. Обернена конгруентна послідовність

$$X_{n+1} = (aX_n^{-1} + c) \bmod 2^e, X_0 = 1, e \geq 3$$

має період 2^{e-1} , якщо $a \bmod 4 = 1$ і $c \bmod 4 = 2$.

Обрані коефіцієнти:

- $X_0 = 42949672$;
- $m = 4294967197$;
- $c = 4294967291$;
- $a = 4294967157$.

Результат роботи:

```
C:\WINDOWS\system32\cmd.exe
Enter index of method (from 1 to 10 or q): 4
Chose one of the presets, or enter own numbers:
1) m4_32b
2 or d) m4_p
a) Own numbers
:d
Enter number of elements: 1000
Interval | Frequency
[0.00;0.10) 0.10
[0.10;0.20) 0.10
[0.20;0.30) 0.10
[0.30;0.40) 0.10
[0.40;0.50) 0.10
[0.50;0.60) 0.09
[0.60;0.70) 0.10
[0.70;0.80) 0.10
[0.80;0.90) 0.10
[0.90;1.00) 0.11
Enter index of method (from 1 to 10 or q):
```

5. Метод об'єднання

$$Z_n = (X_n - Y_n) \bmod m,$$
$$0 \leq X_n < m, \quad 0 \leq Y_n < m' \leq m,$$
$$U_{n+1} = \frac{X_{n+1}}{m}, \quad n \geq 0.$$

Обрані коефіцієнти:

- $m = 4294967197$;
- Послідовність X (другий метод):
 - $X_0 = 42949672$;
 - $m = 4294967291$;
 - $c = 4294967279$;
 - $d = 4294967231$;
 - $a = 4294967197$.
- Послідовність Y (четвертий метод):
 - $X_0 = 42949672$;
 - $m = 4294967197$;
 - $c = 4294967291$;
 - $a = 4294967157$.

Результат роботи:

```
C:\Users\mario\Documents\Documents\University\OOP\LABS\LAB1\x64\Release\LAB1.exe
Enter index of method (from 1 to 10 or q): 5
Chose one of the presets, or enter own numbers:
1 or d) m5_p
o) Own numbers
:b
Chose one of the presets, or enter own numbers:
1 or d) m5_p
o) Own numbers
:d
Enter number of elements: 1000
Interval | Frequency
[0.00;0.10) 0.10
[0.10;0.20) 0.10
[0.20;0.30) 0.10
[0.30;0.40) 0.12
[0.40;0.50) 0.13
[0.50;0.60) 0.10
[0.60;0.70) 0.09
[0.70;0.80) 0.08
[0.80;0.90) 0.09
[0.90;1.00) 0.09
Enter index of method (from 1 to 10 or q): _
```

2. Опис методів генерування нормально розподілених чисел

$$N(0,1): F(x) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^x e^{-\frac{t^2}{2}} dt$$

6. Правило «3-сігма»

$$X_n = m + (sum - 6)\sigma,$$

де m – медіана, σ – дисперсія, sum – сума дванадцяти випадкових чисел, рівномірно розподілених на інтервалі $[a, b]$. Якщо $[a, b] = [0; 1]$, то $m = 0$, а $\sigma = 1$. Правило 3-сігма стверджує, на проміжку $[m-3\sigma; m+3\sigma]$ міститься 99,7% всіх випадкових чисел, що мають розподіл $N(m, \sigma^2)$. Отже для побудови гістограми розподілу $N(0,1)$ достатньо обмежитись інтервалом $[-3;3]$.

Обрані коефіцієнти:

- Рівномірний розподіл за четвертим методом.
- $m = 0$;
- $\sigma = 1$.

Результат роботи:

```
C:\Users\mario\Documents\Documents\University\OOP\LABS\LAB1\x64\Release\LAB1.exe
Enter index of method (from 1 to 10 or q): 6
Chose one of the presets, or enter own numbers:
1 or d) m6_p
o) Own numbers
:d
Enter number of elements: 1000
Interval | Frequency
[-3.00;-2.40) 0.01
[-2.40;-1.80) 0.03
[-1.80;-1.20) 0.07
[-1.20;-0.60) 0.15
[-0.60; 0.00) 0.23
[ 0.00; 0.60) 0.23
[ 0.60; 1.20) 0.17
[ 1.20; 1.80) 0.07
[ 1.80; 2.40) 0.03
[ 2.40; 3.00) 0.01
Enter index of method (from 1 to 10 or q):
```

7. Метод полярних координат

7.1. Нехай U_1 і U_2 – випадкові числа, взяті із генеральної сукупності всіх чисел, рівномірно розподілених на інтервалі $[0; 1]$. Виконати такі перетворення.

$$V_1 \leftarrow 2U_1 - 1,$$

$$V_2 \leftarrow 2U_2 - 1.$$

Числа V_1 і V_2 належать генеральній сукупності чисел, рівномірно розподілених на інтервалі $[-1; 1]$.

7.2. $S \leftarrow V_1^2 + V_2^2.$

7.3. Якщо $S \geq 1$, виконати пункти 7.1 і 7.2.

7.4. Виконати такі перетворення.

$$X_1 \leftarrow V_1 \sqrt{\frac{-2 \ln S}{S}},$$

$$X_2 \leftarrow V_2 \sqrt{\frac{-2 \ln S}{S}}.$$

7.5. Видати числа X_1 і X_2 .

Результат роботи:

```
C:\Users\mario\Documents\Documents\University\OOP\LABS\LAB1\64\Release\LAB1.exe
Enter index of method (from 1 to 10 or q): 7
Chose one of the presets, or enter own numbers:
1 or d) m7_p
o) Own numbers
:d
Enter number of elements: 1000
Interval | Frequency
[-3.00;-2.40) 0.00
[-2.40;-1.80) 0.02
[-1.80;-1.20) 0.07
[-1.20;-0.60) 0.17
[-0.60; 0.00) 0.25
[ 0.00; 0.60) 0.26
[ 0.60; 1.20) 0.17
[ 1.20; 1.80) 0.05
[ 1.80; 2.40) 0.01
[ 2.40; 3.00) 0.00
Enter index of method (from 1 to 10 or q):
```


8. Метод співвідношень

8.1. Згенерувати дві незалежні випадкові величини, рівномірно розподілені на інтервалі $[0; 1]$: $U \neq 0$ і V .

$$X \leftarrow \sqrt{\frac{8}{e}} \frac{V - \frac{1}{2}}{U}.$$

8.2.

8.3. (Необов'язкова перевірка верхньої грані.) Якщо $X^2 \leq 5 - 4e^{\frac{1}{4}}U$, то результатом є число X . Завершити алгоритм.

8.4. (Необов'язкова перевірка нижньої грані.) Якщо $X^2 \geq \frac{4e^{-135}}{U} + 1.4$, то повернутися на крок 8.1.

8.5. (Остаточна перевірка.) Якщо $X^2 \leq -4 \ln U$, то видати число X і завершити алгоритм, інакше повернутися на крок 8.1.

Обрані випадкові послідовності:

- Послідовність U (перший метод).
- Послідовність V (четвертий метод).

Результат роботи:

```
C:\Users\mario\Documents\Documents\University\OOP\LABS\LAB1\x64\Release\LAB1.exe
Enter index of method (from 1 to 10 or q): 8
Chose one of the presets, or enter own numbers:
1 or d) m8_p
o) Own numbers
:d
Enter number of elements: 1000
Interval | Frequency
[-3.00; -2.40) 0.01
[-2.40; -1.80) 0.03
[-1.80; -1.20) 0.08
[-1.20; -0.60) 0.16
[-0.60; 0.00) 0.21
[ 0.00; 0.60) 0.24
[ 0.60; 1.20) 0.18
[ 1.20; 1.80) 0.07
[ 1.80; 2.40) 0.03
[ 2.40; 3.00) 0.01
Enter index of method (from 1 to 10 or q):
```

3. Опис методів генерування розподілів інших типів

9. Метод логарифму для генерування показового розподілу

$$F(x) = 1 - e^{-\frac{x}{\mu}}, x \geq 0.$$

Якщо $y = F(x) = 1 - e^{-\frac{x}{\mu}}$, то $x = F^{-1}(y) = -\mu \ln(1 - y)$. Таким чином, величина

$$x = -\mu \ln(1 - U),$$

має експоненційний розподіл, якщо число U належить генеральній сукупності випадкових величин, рівномірно розподілених на інтервалі $[0; 1]$. Оскільки величина $1-U$ має той же самий розподіл, формулу можна спростити:

$$x = -\mu \ln(U).$$

Обрані випадкові послідовності:

- Послідовність U (четвертий метод).

Результат роботи:

```
C:\Users\mario\Documents\Documents\University\OOP\LABS\LAB1\64\Release\LAB1.exe
Enter index of method (from 1 to 10 or q): 9
Chose one of the presets, or enter own numbers:
1 or d) m9_p
o) Own numbers
:d
Enter number of elements: 1000
Interval | Frequency
[ 0.00; 10.00) 0.40
[ 10.00; 20.00) 0.23
[ 20.00; 30.00) 0.15
[ 30.00; 40.00) 0.09
[ 40.00; 50.00) 0.06
[ 50.00; 60.00) 0.03
[ 60.00; 70.00) 0.01
[ 70.00; 80.00) 0.01
[ 80.00; 90.00) 0.01
[ 90.00; 100.00) 0.00
Enter index of method (from 1 to 10 or q):
```

10. Метод Аренса для генерування гамма-розподілу порядку $a > 1$

$$F(x) = \frac{1}{\Gamma(a)} \int_0^x t^{a-1} e^{-t} dt, x \geq 0, a > 0.$$

10.1. (Генерування кандидата.) Згенерувати випадкове число U , що належить генеральній сукупності випадкових величин, рівномірно розподілених на інтервалі $[0; 1]$. Виконати операції

$$Y \leftarrow \operatorname{tg}(\pi U),$$

$$X \leftarrow \sqrt{2a-1}Y + a - 1.$$

10.2. (Перша перевірка.) Якщо $X \leq 0$, повернутися на крок 10.1.

10.3. (Остаточна перевірка.) Згенерувати випадкове число V , що належить генеральній сукупності випадкових величин, рівномірно озподілених на інтервалі $[0; 1]$.

Якщо $V > (1+Y^2) \exp\left((a-1) \ln\left(\frac{X}{a-1}\right) - \sqrt{2a-1}Y\right)$, повернутися на крок 10.1.

10.4. Видати число X .

Обрані випадкові послідовності:

- Послідовність U (четвертий метод).

Результат роботи:

```
C:\Users\mario\Documents\Documents\University\OOP\LABS\LAB1\x64\Release\LAB1.exe
Enter index of method (from 1 to 10 or q): 10
Chose one of the presets, or enter own numbers:
1 or d) m10_p
o) Own numbers
:
d
Enter number of elements: 1000
Interval | Frequency
[ 0.00; 10.00) 0.94
[ 10.00; 20.00) 0.03
[ 20.00; 30.00) 0.01
[ 30.00; 40.00) 0.01
[ 40.00; 50.00) 0.00
[ 50.00; 60.00) 0.00
[ 60.00; 70.00) 0.00
[ 70.00; 80.00) 0.00
[ 80.00; 90.00) 0.00
[ 90.00; 100.00) 0.00
Enter index of method (from 1 to 10 or q):
```